# ATTACHMENT A

I. Search Procedure

A. The search warrant will be presented to Sprint Nextel personnel who will identify the accounts and files to be searched, described in Section II, below.

B. Sprint Nextel personnel will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Sprint Nextel personnel will provide the account duplicate to law enforcement personnel.

D. Using technology and techniques reasonable available to them, law enforcement personnel will then search the account duplicate for the records and data to be seized, described in Section III, below.

E. Law enforcement personnel will make an electronic copy of the records and data described in Section III found on the account duplicate ("the seized records data").

F. Law enforcement personnel will then seal the account duplicate and not examine it again without further judicial authorization.

II. Accounts and Files to Be Copied by Sprint Nextel Personnel

A. All stored communications and other files reflecting communications, including but not limited to text messages and short message service (SMS), from January 25, 2009, to the present, to or from the wireless telephone number 774-696-7316 and/or wireless telephone handsets with the following identification numbers: IMSI: 316010015562760, and/or UFMI: 180*170847*1.

B. All of the subscriber's address books or lists of the subscriber's contacts;

C: All transactional information of all activity of the telephone numbers and/or handsets described above in Section II(a), whether transmitted to or from a wireless telephone handset associated with the subscriber's account, including messaging logs, other log files, dates, times, methods of connecting, and/or locations. Messaging logs should contain the following information:

i. date of message;
ii. time of message;
iii. source of the message (e.g., the IMEI, IMSI, MEID, and/or ESN associated with the handset from which the message originated, the telephone

number associated with that handset, and the provider associated with that handset); and

iv. destination of the message (e.g., the IMEI, IMSI, MEID, and/or ESN associated with the handset to which the message was sent, the telephone number associated with that handset, and the provider associated with that handset);

D. All business records and subscriber information, in any form kept, pertaining to the telephone numbers and/or handsets described above in Section II(a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and

E. All records indicating the services available to subscribers of the telephone numbers and/or handsets described above in Section II(a).

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. All electronic communications, images, and data, for the period January 25, 2009, to the present, relating to:

violations of 21 U.S.C. § 841(a)(1), 21 U.S.C. § 843(b), and 21 U.S.C. § 846, including but not limited to information about the locations at which RAMOS and others acquire, transport, and store drugs prior to distribution; the times, dates, and locations when and where RAMOS and others acquire narcotics, distribute narcotics; evidence regarding the acquisition, transportation, and distribution of drugs, money, and other proceeds involved in the commission of the above-named offenses; and

B. All of the transactional and other records described in Sections II(B)-(E).